**Jewish Community Day School – Email & Website hack 2017 May.**

**May 9:** Initial e-mail outage. Contacted Google and Register.com after learning (via MX Lookup) that the JCDSRI.org email records had been modified by someone outside of the school to point to a Ukrainian mail server. The school was able to access and modify the mail records at Register.com, so they were restored to their proper state and functionality was restored. Register.com login information was updated and passwords were re-set under the assumption that the change was the result of a compromised Register.com account or hack of Register.com outside of our control (unproven).

**May 19:** Second e-mail outage. Same mail record change to same Ukrainian server. Contacted Rgister.com and learned that the school had lost all control over the JCDSRI.org domain name. Learned the following:

1. **Flashback:** In 2015 when the school moved its website from the old host (Whipple Hill) to the new host (Pin Tight), the JCDSRI.org domain name had the “domain lock protection” which the school had purchased years before temporarily removed. This is normal procedure for Register.com as it allows for them to modify the account when changes are requested by its owner.
2. Register.com did NOT restore “domain lock protection” immediately after modifications were made, which is NOT standard protocol. BIG MISTAKE. The JCDSRI.org account remained in a "volatile state" WITHOUT “domain lock protection,” yet the school’s account showed as “locked.” To our eyes, everything was good, when, in fact, it was not.
3. **Flashback:** During **April 1-4** time period, the JCDSRI.org domain name registration expired due to a lack of response from the school. Expiration warnings were being sent by Register.com to a defunct email address set up by Alan Harlam in 2006. Domain lock protection was supposedly on, so we were given a 30 day grace period to renew the domain before JCDSRI.org was put up for auction. After noticing that there were problems, and investigation was launched and the school discovered that the domain name had expired, but only 3 days into the 30-day protection period offered by “domain lock protection.” The JCDSRI.org domain name was paid for and renewed for three years, and the account showed as up-to-date, locked and owned by the school through 2021.
4. **May 19th:** Seeing as the JCDSRI.org domain name had been erroneously left in a “volatile state” by Register.com back in 2015, the domain name was not protected by “domain lock” as it should have been, and was immediately put up for auction and **legally** acquired by a Ukrainian entity operating through a Panamanian front.
5. The chaotic and previously inexplicable email outages that occurred during the May 9-19 period reflected the school’s gradual loss of control of JCDSRI.org to its new legal owners. By May 19th, all control was lost by the school.

**May 20-24:** Working with Register.com and Google, the school’s online assets were transferred to the newly acquired JCDSRI.com address. Legal counsel was sought out. Functionality was restored to the school under the new domain name and email, documents, calendars and contacts were securely available again. The JCDSRI.com website was activated. Critical financial institutions were notified of the identity violation, as were the faculty, staff and, eventually, the greater community. A presentation with Q&A was provided to the entire school so that everyone would be familiar with the changes, why they were happening, what was at stake, and how to protect themselves and the JCDSRI community.

During this response period, persistent malicious attempts were made by the current owners of JCDSRI.org to gain access to the school’s Google services. The JCDSRI.org website was “scraped,” i.e. an exact copy of the original was made by its new owners; one that is completely under the malicious control of its owners but appears to be genuine, save for being at the compromised JCDSRI.org address. Seeing as intellectual property has been stolen and is being misused by the owners of JCDSRI.org, legal action is now possible with ICANN (Internet Corporation for Assigned Names and Numbers) and Google to potentially re-gain control over the JCDSRI.org domain name or to de-list it from Google searches as fraudulent if this is not possible.

**Today:** All JCDSRI Google services are completely cut off from potential compromise, and full online functionality has been restored to the school. The JCDSRI.com website is fully functional and secure. Secondary and tertiary accounts that use the old JCDSRI.org email addresses for login purposes are being changed by their respective account holders. The fallout continues, but the worst is over re: possible identity theft. More details will be forthcoming on a daily basis.

**Author: David Vernaglia**

**Everlasting Designs, Inc.**

**401-524-6987**

**david@everlastingdesigns.com**